

## PCT COOPERATION TREATY

PCT

NOTIFICATION OF THE RECORDING  
OF A CHANGE(PCT Rule 92bis.1 and  
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

JOSTARNDT, Hans-Dieter  
Brüsseler Ring 51  
52074 Aachen  
ALLEMAGNE

Date of mailing (day/month/year) 18 mars 2002 (18.03.02)	<b>IMPORTANT NOTIFICATION</b>
Applicant's or agent's file reference ACDPA5002PWO	
International application No. PCT/DE00/03506	International filing date (day/month/year) 05 octobre 2000 (05.10.00)

1. The following indications appeared on record concerning:	
<input type="checkbox"/> the applicant	<input type="checkbox"/> the inventor
<input checked="" type="checkbox"/> the agent	<input type="checkbox"/> the common representative
Name and Address JOSTARNDT, Hans-Dieter Eupener Strasse 266 52076 Aachen Germany	State of Nationality
	State of Residence
	Telephone No. 49 241 400 71 00
	Facsimile No. 49 241 400 71 21
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:	
<input type="checkbox"/> the person	<input type="checkbox"/> the name
<input checked="" type="checkbox"/> the address	<input type="checkbox"/> the nationality
<input type="checkbox"/> the residence	
Name and Address JOSTARNDT, Hans-Dieter Brüsseler Ring 51 52074 Aachen Germany	State of Nationality
	State of Residence
	Telephone No. 49 241 400 71 00
	Facsimile No. 49 241 400 71 21
3. Further observations, if necessary:	
4. A copy of this notification has been sent to:	
<input checked="" type="checkbox"/> the receiving Office	<input type="checkbox"/> the designated Offices concerned
<input type="checkbox"/> the International Searching Authority	<input checked="" type="checkbox"/> the elected Offices concerned
<input checked="" type="checkbox"/> the International Preliminary Examining Authority	<input type="checkbox"/> other:

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Kari HUYNH-KHUONG
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

**THIS PAGE BLANK (USPTO)**

## PATENT COOPERATION TREATY

PCT

## NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner  
 US Department of Commerce  
 United States Patent and Trademark  
 Office, PCT  
 2011 South Clark Place Room  
 CP2/5C24  
 Arlington, VA 22202  
 ETATS-UNIS D'AMERIQUE  
 in its capacity as elected Office

<b>Date of mailing (day/month/year)</b> 13 September 2001 (13.09.01)	
<b>International application No.</b> PCT/DE00/03506	<b>Applicant's or agent's file reference</b> ACDPA5002PWO
<b>International filing date (day/month/year)</b> 05 October 2000 (05.10.00)	<b>Priority date (day/month/year)</b> 07 October 1999 (07.10.99)
<b>Applicant</b> LANG, Jürgen et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:  
 02 May 2001 (02.05.01)

☐ in a notice effecting later election filed with the International Bureau on:  
 \_\_\_\_\_

2. The election ☒ was  
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

<b>The International Bureau of WIPO</b> 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	<b>Authorized officer</b> Maria KIRCHNER Telephone No.: (41-22) 338.83.38
--	---

**THIS PAGE BLANK (USPTO)**

PCT

## ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Vom Anmeldeamt auszufüllen

Internationales Aktenzeichen

Internationales Anmeldedatum

Name des Anmeldeamts und "PCT International Application"

Aktenzeichen des Anmelders oder Anwalts (falls gewünscht)  
(max. 12 Zeichen) ACDPA5002PWO

## Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Sicherungsmodul und Verfahren zur Erstellung fälschungssicherer Dokumente

## Feld Nr. II ANMELDER

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

DEUTSCHE POST AG  
Heinrich-von-Stephan-Straße 1

D-53175 Bonn

☐ Diese Person ist gleichzeitig Erfinder

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Staatsangehörigkeit (Staat):

Deutschland

Sitz oder Wohnsitz (Staat):

Deutschland

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika☐ nur die Vereinigten Staaten von Amerika☐ die im Zusatzfeld angegebenen Staaten

## Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

LANG, Jürgen  
Schau ins Land 15

D-51429 Bergisch Gladbach

Diese Person ist:

☐ nur Anmelder☒ Anmelder und Erfinder☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat):

Deutschland

Sitz oder Wohnsitz (Staat):

Deutschland

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika☒ nur die Vereinigten Staaten von Amerika☐ die im Zusatzfeld angegebenen Staaten☒ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

## Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER; ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als:

☒ Anwalt☐ gemeinsamer Vertreter

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)

JOSTARNDT, Hans-Dieter  
Eupener Straße 266D-52076 Aachen  
Deutschland

Telefonnr.:

(++49)241/54 32 13

Telefaxnr.:

(++49)241/543240

Fernschreibnr.:

☐ Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

**THIS PAGE BLANK (USPTO)**

**Fortsetzung von Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER**

*Wird keines der folgenden Felder benutzt, so ist dieses Blatt dem Antrag nicht beizufügen.*

Name und Anschrift: (Familiennamen, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

MEYER, Bernd  
Zum Stöckerhof 2 c

D-53639 Königswinter

Diese Person ist:

☐ nur Anmelder

☒ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat): Deutschland

Sitz oder Wohnsitz (Staat): Deutschland

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☒ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: (Familiennamen, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

Diese Person ist:

☐ nur Anmelder

☐ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☐ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: (Familiennamen, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

Diese Person ist:

☐ nur Anmelder

☐ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☐ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: (Familiennamen, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

Diese Person ist:

☐ nur Anmelder

☐ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☐ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem zusätzlichen Fortsetzungsblatt angegeben.

**THIS PAGE BLANK (USPTO)**



## Feld Nr. V BESTIMMUNG STAATEN

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen (bitte die entsprechenden Kästchen ankreuzen; wenigstens ein Kästchen muß angekreuzt werden):

## Regionales Patent

- ☒ AP ARIPO-Patent: GH Ghana, GM Gambia, KE Kenia, LS Lesotho, MW Malawi, SD Sudan, SZ Swasiland, UG Uganda, ZW Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist
- ☒ EA Eurasisches Patent: AM Armenien, AZ Aserbaidshan, BY Belarus, KG Kirgisistan, KZ Kasachstan, MD Republik Moldau, RU Russische Föderation, TJ Tadschikistan, TM Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist
- ☒ EP Europäisches Patent: AT Österreich, BE Belgien, CH und LI Schweiz und Liechtenstein, DE Deutschland, DK Dänemark, ES Spanien, FI Finnland, FR Frankreich, GB Vereinigtes Königreich, GR Griechenland, IE Irland, IT Italien, LU Luxemburg, MC Monaco, NL Niederlande, PT Portugal, SE Schweden und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist
- ☒ OA OAPI-Patent: BF Burkina Faso, BJ Benin, CF Zentralafrikanische Republik, CG Kongo, CI Côte d'Ivoire, CM Kamerun, GA Gabun, GN Guinea, ML Mali, MR Mauretanien, NE Niger, SN Senegal, TD Tschad, TG Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist (falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)

Nationales Patent (falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben):

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> AL Albanien                          | <input checked="" type="checkbox"/> LT Litauen   |
| <input checked="" type="checkbox"/> AM Armenien                          | <input checked="" type="checkbox"/> LU Luxemburg                                       |
| <input checked="" type="checkbox"/> AT Österreich                        | <input checked="" type="checkbox"/> LV Lettland  |
| <input checked="" type="checkbox"/> AU Australien                        | <input checked="" type="checkbox"/> MD Republik Moldau                                 |
| <input checked="" type="checkbox"/> AZ Aserbaidshan                      | <input checked="" type="checkbox"/> MG Madagaskar                                      |
| <input checked="" type="checkbox"/> BA Bosnien-Herzegowina               | <input checked="" type="checkbox"/> MK Die ehemalige jugoslawische Republik Mazedonien |
| <input checked="" type="checkbox"/> BB Barbados                          | <input checked="" type="checkbox"/> MN Mongolei  |
| <input checked="" type="checkbox"/> BG Bulgarien                         | <input checked="" type="checkbox"/> MW Malawi  |
| <input checked="" type="checkbox"/> BR Brasilien                         | <input checked="" type="checkbox"/> MX Mexiko  |
| <input checked="" type="checkbox"/> BY Belarus                           | <input checked="" type="checkbox"/> NO Norwegen  |
| <input checked="" type="checkbox"/> CA Kanada                            | <input checked="" type="checkbox"/> NZ Neuseeland                                      |
| <input checked="" type="checkbox"/> CH und LI Schweiz und Liechtenstein  | <input checked="" type="checkbox"/> PL Polen   |
| <input checked="" type="checkbox"/> CN China                             | <input checked="" type="checkbox"/> PT Portugal  |
| <input checked="" type="checkbox"/> CU Kuba                              | <input checked="" type="checkbox"/> RO Rumänien  |
| <input checked="" type="checkbox"/> CZ Tschechische Republik             | <input checked="" type="checkbox"/> RU Russische Föderation                            |
| <input checked="" type="checkbox"/> DE Deutschland                       | <input checked="" type="checkbox"/> SD Sudan   |
| <input checked="" type="checkbox"/> DK Dänemark                          | <input checked="" type="checkbox"/> SE Schweden  |
| <input checked="" type="checkbox"/> EE Estland                           | <input checked="" type="checkbox"/> SG Singapur  |
| <input checked="" type="checkbox"/> ES Spanien                           | <input checked="" type="checkbox"/> SI Slowenien                                       |
| <input checked="" type="checkbox"/> FI Finnland                          | <input checked="" type="checkbox"/> SK Slowakei  |
| <input checked="" type="checkbox"/> GB Vereinigtes Königreich            | <input checked="" type="checkbox"/> SL Sierra Leone                                    |
| <input checked="" type="checkbox"/> GE Georgien                          | <input checked="" type="checkbox"/> TJ Tadschikistan                                   |
| <input checked="" type="checkbox"/> GH Ghana                             | <input checked="" type="checkbox"/> TM Turkmenistan                                    |
| <input checked="" type="checkbox"/> GM Gambia                            | <input checked="" type="checkbox"/> TR Türkei  |
| <input checked="" type="checkbox"/> GW Guinea-Bissau                     | <input checked="" type="checkbox"/> TT Trinidad und Tobago                             |
| <input checked="" type="checkbox"/> HU Ungarn                            | <input checked="" type="checkbox"/> UA Ukraine   |
| <input checked="" type="checkbox"/> ID Indonesien                        | <input checked="" type="checkbox"/> UG Uganda  |
| <input checked="" type="checkbox"/> IL Israel                            | <input checked="" type="checkbox"/> US Vereinigte Staaten von Amerika                  |
| <input checked="" type="checkbox"/> IS Island                            | <input checked="" type="checkbox"/> UZ Usbekistan                                      |
| <input checked="" type="checkbox"/> JP Japan                             | <input checked="" type="checkbox"/> VN Vietnam   |
| <input checked="" type="checkbox"/> KE Kenia                             | <input checked="" type="checkbox"/> YU Jugoslawien                                     |
| <input checked="" type="checkbox"/> KG Kirgisistan                       | <input checked="" type="checkbox"/> ZW Simbabwe  |
| <input checked="" type="checkbox"/> KP Demokratische Volksrepublik Korea |  |
| <input checked="" type="checkbox"/> KR Republik Korea                    |  |
| <input checked="" type="checkbox"/> KZ Kasachstan                        |  |
| <input checked="" type="checkbox"/> LC Saint Lucia                       |  |
| <input checked="" type="checkbox"/> LK Sri Lanka                         |  |
| <input checked="" type="checkbox"/> LR Liberia                           |  |
| <input checked="" type="checkbox"/> LS Lesotho                           |  |

Kästchen für die Bestimmung von Staaten (für die Zwecke eines nationalen Patents), die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind:

- ☒ .....
- ☐ .....
- ☐ .....

Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der Bestimmung von .....

Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. (Die Bestätigung einer Bestimmung erfolgt durch die Einreichung einer Mitteilung, in der diese Bestimmung angegeben wird, und die Zahlung der Bestimmungs- und der Bestätigungsgebühr. Die Bestätigung muß beim Anmeldeamt innerhalb der Frist von 15 Monaten eingehen.)

**THIS PAGE BLANK (USPTO)**

**Feld Nr. VI PRIORITÄTSANTRAG**Weitere Prioritätsanträge sind im Zusatzfeld angegeben. ☐

Die Priorität der folgenden früheren Anmeldung(en) wird hiermit beansprucht:

Staat (Anmelde- oder Bestimmungsstaat der Anmeldung)	Anmeldedatum (Tag/Monat/Jahr)	Aktenzeichen	Anmeldeamt (nur bei regionaler oder internationaler Anmeldung)
(1) Deutschland	27.04.2000 (27. April 2000)	100 20 561.5-31	
(2) Deutschland	07.10.1999 (07. Oktober 1999)	199 48 319.1	
(3)			

Dieses Kästchen ankreuzen, wenn die beglaubigte Kopie der früheren Anmeldung von dem Amt ausgestellt werden soll, das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist (eine Gebühr kann verlangt werden):

☒ Das Anmeldeamt wird hiermit ersucht, eine beglaubigte Abschrift der oben in Zeile(n) 1,2 bezeichneten früheren Anmeldung(en) zu erstellen und dem Internationalen Büro zu übermitteln.
**Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE**

Wahl der Internationalen Recherchenbehörde (ISA) (Sind zwei oder mehr Internationale Recherchenbehörden für die internationale Recherche zuständig, ist der Name der Behörde anzugeben, die die internationale Recherche durchführen soll; Zweibuchstaben-Code genügt):

ISA /

Frühere Recherche Auszufüllen, wenn eine Recherche (internationale Recherche, Recherche internationaler Art oder sonstige Recherche) bereits bei der internationalen Recherchenbehörde beantragt oder von ihr durchgeführt worden ist und diese Behörde nun ersucht wird, die internationale Recherche soweit wie möglich auf die Ergebnisse einer solchen früheren Recherche zu stützen. Die Recherche oder der Recherchenantrag ist durch Angabe der betreffenden Anmeldung (bzw. deren Übersetzung) oder des Recherchenantrags zu bezeichnen.

Staat (oder regionales Amt):

Datum (Tag/Monat/Jahr):

Aktenzeichen:

**Feld Nr. VIII KONTROLLISTE**

Diese internationale Anmeldung umfaßt:

1. Antrag : 4 Blätter  
 2. Beschreibung : 16 Blätter  
 3. Ansprüche : 5 Blätter  
 4. Zusammenfassung : 1 Blätter  
 5. Zeichnungen : 1 Blätter  
 Insgesamt : 27 Blätter

Dieser internationalen Anmeldung liegen die nachstehend angekreuzten Unterlagen bei:

1. ☐ Unterzeichnete gesonderte Vollmacht  
 2. ☐ Kopie der allgemeinen Vollmacht  
 3. ☐ Begründung für das Fehlen der Unterschrift  
 4. ☐ Prioritätsbeleg(e) (durch die Zeilennummer von Feld Nr. VI kennzeichnen):  
 5. ☒ Blatt für die Gebührenberechnung  
 6. ☐ Gesonderte Angaben zu hinterlegten Mikroorganismen  
 7. ☐ Sequenzprotokolle für Nucleotide und/oder Aminosäuren (Diskette)  
 8. ☐ Sonstige (einzeln auflisten):

Abbildung Nr. 1 der Zeichnungen (falls vorhanden) soll mit der Zusammenfassung veröffentlicht werden.**Feld Nr. IX UNTERSCHRIFT DES ANMELDERS ODER DES ANWALTS**

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

*Hans-Dieter Jostardt*  
 Dr. Hans-Dieter Jostardt  
 - Patentanwalt -

Vom Anmeldeamt auszufüllen

1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung:	2. Zeichnungen <input type="checkbox"/> eingegangen:  <input type="checkbox"/> nicht eingegangen:
3. Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:	
4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT:	
5. Vom Anmelder benannte Internationale Recherchenbehörde: ISA /	6. <input type="checkbox"/> Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchegebühr aufgeschoben

Vom Internationalen Büro auszufüllen

Datum des Eingangs des Aktenexemplars beim Internationalen Büro:

**THIS PAGE BLANK (USPTO)**

# PCT

## BLATT FÜR DIE GEBÜHRENBERECHNUNG

### Anhang zum Antrag

Von Anmeldeamt auszufüllen

Internationales Aktenzeichen

Aktenzeichen des Anmelders  
oder Anwalts ACDPA5002PWO

Eingangsstempel des Anmeldeamts

Anmelder  
DEUTSCHE POST AG, Heinrich-von-Stephan-Straße 1, D-53175 Bonn

### BERECHNUNG DER VORGESCHRIEBENEN GEBÜHREN

1. ÜBERMITTLUNGSGEBÜHR . . . . . 175,00 T

2. RECHERCHENGEBÜHR . . . . . 1848,26 S

Die internationale Recherche ist durchzuführen von  
(Sind zwei oder mehr Internationale Recherchenbehörden für die internationale Recherche zuständig,  
ist der Name der Behörde anzugeben, die die internationale Recherche durchführen soll.)

### 3. INTERNATIONALE GEBÜHR

#### Grundgebühr

Die internationale Anmeldung enthält 27 Blätter.

umfaßt die ersten 30 Blätter . . . . . 799,93 b<sub>1</sub>

\_\_\_\_\_ x \_\_\_\_\_ = \_\_\_\_\_ b<sub>2</sub>

Anzahl der Blätter Zusatzblattgebühr  
über 30

Addieren Sie die in Feld b<sub>1</sub> und b<sub>2</sub> eingetragenen  
Beträge, und tragen Sie die Summe in Feld B ein . . . . . 799,93 B

#### Bestimmungsgebühren

Die internationale Anmeldung enthält 8 Bestimmungen.

172,11 x 8 = 1376,88 D

Anzahl der zu zahlenden Bestimmungsgebühr

Bestimmungsgebühren (maximal 11)

Addieren Sie die in Feld B und D eingetragenen

Beträge, und tragen Sie die Summe in Feld I ein . . . . . 2176,81 I

(Anmelder aus einigen Staaten haben Anspruch auf eine Ermäßigung der internationalen Gebühr um  
75%. Hat der Anmelder (oder haben alle Anmelder) einen solchen Anspruch, so beträgt der in Feld I  
einzutragende Gesamtbetrag 25% der Summe der in Feld B und D eingetragenen Beträge.)

4. GEBÜHR FÜR PRIORITÄTSBELEG . . . . . 58,00 P

### 5. GESAMTBETRAG DER ZU ZAHLENDEN GEBÜHREN

Addieren Sie die in Feldern T, S, I und P eingetragenen Beträge,  
und tragen Sie die Summe in das nebenstehende Feld ein . . . . . 4258,07

INSGESAMT

☐ Die Bestimmungsgebühren werden jetzt noch nicht gezahlt.

### ZAHLUNGSWEISE

☒ Abbuchungsauftrag (siehe unten) ☐ Bankwechsel ☐ Kupons  
☐ Scheck ☐ Barzahlung ☐ Sonstige (einzeln angeben):  
☐ Postanweisung ☐ Gebührenmarken

### ABBUCHUNGSauftrag (diese Zahlungsweise gibt es nicht bei allen Anmeldeämtern)

Das Anmeldeamt/ DPA

- ☒ wird beauftragt, den vorstehend angegebenen Gesamtbetrag der Gebühren von meinem laufenden Konto abzubuchen.  
☒ wird beauftragt, Fehlbeträge oder Überzahlungen des vorstehend angegebenen Gesamtbetrags der Gebühren meinem laufenden Konto zu belasten bzw. gutzuschreiben.  
☒ wird beauftragt, die Gebühr für die Ausstellung des Prioritätsbelegs und seine Übermittlung an das Internationale Büro der WIPO von meinem laufenden Konto abzubuchen.

3 410 651 00

Kontonummer

04. Oktober 2000

Datum (Tag/Monat/Jahr)

Unterschrift

**THIS PAGE BLANK (USPTO)**

"Express Mail" mailing label  
number EL 928737461

Date of Deposit  
- APRIL 02, 2002 -

I hereby certify that this paper or fee is  
being deposited with the United States Postal  
Service "Express Mail Post Office to  
Addressee" service under 37CFR 1.10 on the  
date indicated above and is addressed to **BOX**  
**PaCCT**, Commissioner for Patents,  
Washington, D.C. 20231

-J. Lynn Ferry-

(Typed or printed name of person mailing  
paper or fee)

(Signature of person mailing paper or fee)

Der Antrag ist bei der zuständigen mit der internationalen vorläufigen Prüfung beauftragten Behörde oder, wenn zwei oder mehr Behörden zuständig sind, bei der vom Anmelder gewählten Behörde einzureichen. Der Anmelder kann den Namen oder den Zweibuchstaben-Code der Behörde auf der nachstehenden Zeile angeben.

IPEA/

## PCT

## KAPITEL II

## ANTRAG AUF INTERNATIONALE VORLÄUFIGE PRÜFUNG

nach Artikel 31 des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens:  
Der (die) Unterzeichnete(n) beantragt (beantragen), daß für die nachstehend bezeichnete internationale Anmeldung die internationale vorläufige Prüfung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens durchgeführt wird.

Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen

Bezeichnung der IPEA

Eingangsdatum des ANTRAGS

## Feld Nr. I KENNZEICHNUNG DER INTERNATIONALEN ANMELDUNG

Aktenzeichen des Anmelders oder Anwalts

ACDPA5002PWO

Internationales Aktenzeichen

PCT/DE00/03506

Internationales Anmeldedatum (Tag/Monat/Jahr)

05. Oktober 2000 (05.10.2000)

(Frühester) Prioritätstag (Tag/Monat/Jahr)

07. Oktober 1999 (07.10.1999)

Bezeichnung der Erfindung Sicherungsmodul und Verfahren zur Erstellung fälschungssicherer Dokumente

## Feld Nr. II ANMELDER

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)

DEUTSCHE POST AG  
Heinrich-von-Stephan-Straße 1

D-53175 Bonn

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Staatsangehörigkeit (Staat):

Deutschland

Sitz oder Wohnsitz (Staat):

Deutschland

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)

LANG, Jürgen  
Schau ins Land 15

D-51429 Bergisch Gladbach

Staatsangehörigkeit (Staat):

Deutschland

Sitz oder Wohnsitz (Staat):

Deutschland

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)

MEYER, Bernd  
Zum Stöckerhof 2 c

D-53639 Königswinter

Staatsangehörigkeit (Staat):

Deutschland

Sitz oder Wohnsitz (Staat):

Deutschland

☐ Weitere Anmelder sind auf einem Fortsetzungsblatt angegeben.

**THIS PAGE BLANK (USPTO)**



**Feld Nr. III ANWALT ODER GEMEINSAMER VERTRETER; ZUSTELLANSCHRIFT**

Die folgende Person ist ☒ Anwalt ☐ gemeinsamer Vertreter  
 und ☒ ist vom (von den) Anmelder(n) bereits früher bestellt worden und vertritt ihn (sie) auch für die internationale vorläufige Prüfung.  
☐ wird hiermit bestellt; eine etwaige frühere Bestellung eines Anwalts/gemeinsamen Vertreters wird hiermit widerrufen.  
☐ wird hiermit zusätzlich zu dem bereits früher bestellten Anwalt/gemeinsamen Vertreter, nur für das Verfahren vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde bestellt.

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*

JOSTARNDT, Hans-Dieter  
Eupener Straße 266

52076 Aachen  
Deutschland

Telefonnr.:

(++49)241/543213

Telefaxnr.:

(++49)241/543240

Fernschreibnr.:

☐ Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben wird.

**Feld Nr. IV ERKLÄRUNG BETREFFEND ÄNDERUNGEN**

Der Anmelder wünscht, daß die mit der internationalen vorläufigen Prüfung beauftragte Behörde\*

- i) ☒ die internationale vorläufige Prüfung auf der Grundlage der internationalen Anmeldung in der ursprünglich eingereichten Fassung aufnimmt.
- ii) ☐ die Änderungen nach Artikel 34  
☐ der Beschreibung (Änderungen liegen bei)  
☐ der Ansprüche (Änderungen liegen bei)  
☐ der Zeichnungen (Änderungen liegen bei)  
 berücksichtigt.
- iii) ☐ die beim Internationalen Büro eingereichten Änderungen der Ansprüche nach Artikel 19 berücksichtigt (Kopie liegt bei).
- iv) ☐ die Änderungen der Ansprüche nach Artikel 19 nicht berücksichtigt, sondern als überholt ansieht.
- v) ☐ den Beginn der internationalen vorläufigen Prüfung bis zum Ablauf von 20 Monaten ab dem Prioritätsdatum aufschiebt, sofern die Behörde nicht eine Kopie nach Artikel 19 vorgenommener Änderungen oder eine Erklärung des Anmelders erhält, daß er keine solchen Änderungen vornehmen will (Regel 69.1 d)). *(Dieses Kästchen darf nur angekreuzt werden, wenn die Frist nach Artikel 19 noch nicht abgelaufen ist.)*

\* Wenn kein Kästchen angekreuzt wird, wird mit der internationalen vorläufigen Prüfung auf der Grundlage der internationalen Anmeldung in der ursprünglich eingereichten Fassung begonnen; wenn eine Kopie der Änderungen der Ansprüche nach Artikel 19 und/oder Änderungen der internationalen Anmeldung nach Artikel 34 bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde eingeht, bevor diese mit der Erstellung eines schriftlichen Bescheids oder des internationalen vorläufigen Prüfungsberichts begonnen hat, wird jedoch die geänderte Fassung verwendet.

**Feld Nr. V BENENNUNG VON STAATEN ALS AUSGEWÄHLTE STAATEN**

☒ Der Anmelder benennt als ausgewählte Staaten alle auswählbaren Staaten (das heißt, alle Staaten, die bestimmt wurden und durch Kapitel II des PCT gebunden sind) ausgenommen .....

*(Möchte der Anmelder bestimmte Staaten nicht auswählen, sind die Namen oder Zweibuchstaben-Codes dieser Staaten auf den obenstehenden Zeilen anzugeben.)*

**THIS PAGE BLANK (USPTO)**

## Feld Nr. VI KONTROLLISTE

Dem Antrag liegen folgende Unterlagen für die Zwecke der internationalen vorläufigen Prüfung bei:

## 1. Änderungen nach Artikel 34

Beschreibung	:	Blätter
Ansprüche	:	Blätter
Zeichnungen	:	Blätter

## 2. Begleitschreiben zu den Änderungen nach Artikel 34

: Blätter

## 3. Kopie der Änderungen nach Artikel 19

: Blätter

## 4. Kopie einer Erklärung nach Artikel 19

: Blätter

## 5. Sonstige (einzeln aufführen):

: Blätter

Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen

erhalten nicht erhalten

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Dem Antrag liegen außerdem die nachstehend angekreuzten Unterlagen bei:

1. ☐ unterzeichnete gesonderte Vollmacht4. ☒ Blatt für die Gebührenberechnung2. ☐ Kopie der allgemeinen Vollmacht5. ☐ sonstige (einzeln aufführen):3. ☐ Begründung für das Fehlen der Unterschrift

## Feld Nr. VII UNTERSCHRIFT DES ANMELDERS, ANWALTS ODER GEMEINSAMEN VERTRETERS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

*O. n. Kam. Diele Jostardt*  
 JOSTARNDT, Hans-Dieter  
 - Patentanwalt -  
 European Patent Attorney, No.: 093250

Aachen, 02. Mai 2001

Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen

1. Datum des tatsächlichen Eingangs des ANTRAGS:

2. Geändertes Eingangsdatum des Antrags aufgrund von BERICHTIGUNGEN nach Regel 60.1.b):

3. ☐ Eingangsdatum des Antrags NACH Ablauf von 19 Monaten ab Prioritätsdatum; Punkt 4 und Punkt 5, unten, finden keine Anwendung.☐ Der Anmelder wurde entsprechend unterrichtet4. ☐ Eingangsdatum des Antrags INNERHALB 19 Monate ab Prioritätsdatum wegen Fristverlängerung nach Regel 80.5.5. ☐ Das Eingangsdatum des Antrags liegt nach Ablauf von 19 Monaten ab Prioritätsdatum, der verspätete Eingang ist aber nach Regel 82 ENTSCHULDIGT.

Vom Internationalen Büro auszufüllen

Antrag vom IPEA erhalten am:

**THIS PAGE BLANK (USPTO)**

# PCT

## KAPITEL II

### BLATT FÜR DIE GEBÜHRENBERECHNUNG

#### Anlage zum Antrag auf internationale vorläufige Prüfung

Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen

Internationales Aktenzeichen **PCT/DE00/03506**

Aktenzeichen des Anmelders oder Anwalts **ACDPA5002PWO**

Eingangsstempel der IPEA

Anmelder **DEUTSCHE POST AG, Heinrich-von-Stephan-Straße 1, D-53175 Bonn**

#### Berechnung der vorgeschriebenen Gebühren

1. Gebühr für die vorläufige Prüfung ..... **2998,29** **P**

2. Bearbeitungsgebühr (Anmelder aus einigen Staaten haben Anspruch auf eine Ermäßigung der Bearbeitungsgebühr um 75%. Hat der Anmelder (oder haben alle Anmelder) einen solchen Anspruch, so beträgt der in Feld H einzutragende Betrag 25 % der Bearbeitungsgebühr.) ..... **287,51** **H**

3. Gesamtbetrag der vorgeschriebenen Gebühren  
Addieren Sie die Beträge in den Feldern P und H und tragen Sie die Summe in das nebenstehende Feld ein ..... **3285,80**  
**INSGESAMT**

#### Zahlungsart

☐ Abbuchungsauftrag für das laufende Konto bei der IPEA (siehe unten)

☐ Scheck

☐ Postanweisung

☐ Bankwechsel

☐ Barzahlung

☐ Gebührenmarken

☐ Kupons

☒ Sonstige (einzeln angeben):  
Überweisung

#### Abbuchungsauftrag (diese Zahlungsweise gibt es nicht bei allen Behörden)

Die IPEA/ \_\_\_\_\_ ☐ wird beauftragt, den vorstehend angegebenen Gesamtbetrag der Gebühren von meinem laufenden Konto abzubuchen.

☐ (dieses Kästchen darf nur angekreuzt werden, wenn die Vorschriften der IPEA über laufende Konten dieses Verfahren erlauben) wird beauftragt, Fehlbeträge oder Überzahlungen des vorstehend angegebenen Gesamtbetrags der Gebühren meinem laufenden Konto zu belasten bzw. gutzuschreiben.

Kontonummer

Datum (Tag/Monat/Jahr)

Unterschrift

*Dr. Hans-Dieter Jochims*

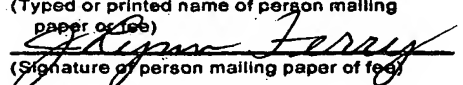
**THIS PAGE BLANK (USPTO)**

"Express Mail" mailing label  
number EL 928737461

Date of Deposit  
- APRIL 02, 2002 -

I hereby certify that this paper or fee is  
being deposited with the United States Postal  
Service "Express Mail Post Office to  
Addressee" service under 37CFR 1.10 on the  
date indicated above and is addressed to **Box**  
**Patents**, Commissioner for Patents,  
Washington, D.C. 20231  
- J. Lynn Ferry -

(Typed or printed name of person mailing  
paper or fee)

  
(Signature of person mailing paper or fee)

## Neue Patentansprüche:

1. Sicherungsmodul zur Erzeugung fälschungssicherer  
5 Dokumente mit den Merkmalen,  
- dass es ein Identifikationsregister, ein  
Schlüsselregister und einen Geheimnisgenerator enthält,  
der ein nicht vorhersehbares Geheimnis erzeugt,  
- dass in einer Kombinationsmaschine (K1) ein  
10 Ausgangswert des Identifikationsregisters und ein  
Ausgangswert des Geheimnisgenerators kombiniert werden,  
- dass der Ausgangswert der Kombinationsmaschine (K1)  
mit einer Verschlüsselungsmaschine verschlüsselt wird,  
- dass der Ausgangswert der Verschlüsselungsmaschine  
15 über ein Auslassventil (1) an eine Bescheinigungsstelle  
ausgegeben wird,  
- dass in einer zweiten Kombinationsmaschine (K2) eine  
Kombination des Geheimnisses und der über ein  
Einlassventil eingegebenen Eingangsdaten erfolgt,  
20 - dass der Ausgangswert der Kombinationsmaschine (K2)  
zur Bildung eines irreversiblen Hash-Wertes herangezogen  
wird und  
- dass der Hash-Wert aus dem Auslassventil (2)  
ausgegeben wird.
- 25
2. Sicherungsmodul nach Anspruch 1, d a d u r c h  
g e k e n n z e i c h n e t, dass die  
Verschlüsselungsmaschine mit einem Schlüsselregister  
verbunden ist, wobei wenigstens ein in dem  
30 Schlüsselregister enthaltener Wert in der  
Verschlüsselungsmaschine zur Verschlüsselung eingesetzt  
werden kann.

**THIS PAGE BLANK (USPTO)**



3. Verwendung des Sicherungsmoduls nach einem oder mehreren der Ansprüche 1 oder 2 in einem Verfahren zur Erstellung
- 5 fälschungssicherer Dokumente, d a d u r c h  
g e k e n n z e i c h n e t, dass die Daten,  
die aus dem zweiten Datenausgang ausgegeben werden als  
fälschungssichere Informationen auf die zu erstellenden  
fälschungssicheren Dokumente ausgegeben werden.

**THIS PAGE BLANK (USPTO)**

"Express Mail" mailing label  
number EL 928737461

Date of Deposit  
- APRIL 02, 2002 -

I hereby certify that this paper or fee is  
being deposited with the United States Postal  
Service "Express Mail Post Office to  
Addressee" service under 37CFR 1.10 on the  
date indicated above and is addressed to Box  
P&C-1, Commissioner for Patents,  
Washington, D.C. 20231

- J. Lynn Ferry -

(Typed or printed name of person mailing  
paper or fee)

  
(Signature of person mailing paper or fee)

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT  
AUF DEM GEBIET DES PATENTWESENS

m.f

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

REC'D 26 OCT 2002

WFO PCT

10/089990

Aktenzeichen des Anmelders oder Anwalts <b>ACDPA5002PW0</b>	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen <b>PCT/DE 00/ 03506</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>05/10/2000</b>	Prioritätsdatum (Tag/Monat/Jahr) <b>07/10/1999</b>
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK <b>G06F1/00</b>		
Anmelder <b>DEUTSCHE POST AG et al.</b>		

1. Der internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser **BERICHT** umfaßt insgesamt 2 Blätter einschließlich dieses Deckblatts.

☐ Außerdem liegen dem Bericht **ANLAGEN** bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsvorschriften zum PCT)

Diese Anlagen umfassen insgesamt \_\_\_\_\_ Blätter.

RECEIVED

3. Dieser Bericht enthält Angaben und die entsprechenden Seiten zu folgenden Punkten:

APR 18 2003

I ☒ Grundlage des Berichts

II ☐ Priorität

Technology Center 2100

III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit

IV ☐ Mangelnde Einheitlichkeit der Erfindung

V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

VI ☐ Bestimmte angeführte Unterlagen


VII ☐ Bestimmte Mängel der internationalen Anmeldung

VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

RECEIVED

APR 18 2003

Technology Center 2600

Datum der Einreichung des Antrags <b>02/05/2001</b>	Datum der Fertigstellung dieses Berichts <b>22/10/2002</b>
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde  Europäisches Patentamt, Gitschiner Str. 103 D-10969 Berlin - Deutschland Tel.: (+49-30) 25901-0 Fax: (+49-30) 25901-840	Bevollmächtigter Bediensteter <b>KURVERS F J J</b> Tel. (+49-89) 2399 2828



**I. Grundlage des Berichts**

Grundlage dieses Berichtes sind die Anmeldungsunterlagen in der ursprünglich eingereichten Fassung.

**V. Begründete Feststellung nach Regel 66.2(a)(ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit**

In Anbetracht der im internationalen Recherchenbericht angeführten Unterlagen wird festgestellt, daß die Erfindung, wie sie in mindestens einigen von den Ansprüchen gekennzeichnet ist, die in Artikel 33(1) PCT aufgeführten Kriterien allem Anschein nach nicht erfüllt, d.h. nicht als neu und/oder auf erfinderischer Tätigkeit beruhend anzusehen ist (siehe internationaler Recherchenbericht, insbesondere die mit X und/oder Y angeführten Unterlagen und die entsprechenden Anspruchsnummern).

Translation

PATENT COOPERATION TREATY

PCT

10/689990

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference ACDPA5002PWO	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE00/03506	International filing date (day/month/year) 05 October 2000 (05.10.00)	Priority date (day/month/year) 07 October 1999 (07.10.99)
International Patent Classification (IPC) or national classification and IPC G07B 17/00		
Applicant DEUTSCHE POST AG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of <u>2</u> sheets, including this cover sheet.  <input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).  These annexes consist of a total of _____ sheets.
3. This report contains indications relating to the following items:  I <input checked="" type="checkbox"/> Basis of the report II <input type="checkbox"/> Priority III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability IV <input type="checkbox"/> Lack of unity of invention V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI <input type="checkbox"/> Certain documents cited VII <input type="checkbox"/> Certain defects in the international application VIII <input type="checkbox"/> Certain observations on the international application

Date of submission of the demand 02 May 2001 (02.05.01)	Date of completion of this report 22 October 2002 (22.10.2002)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

**I. Basis of the report**

The basis of international preliminary examination report is the application as originally filed.

**V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability**

In light of the documents cited in the international search report, it is considered that the invention as defined in at least some of the claims does not appear to meet the criteria mentioned in Article 33(1) PCT, i.e. does not appear to be novel and/or to involve an inventive step (see international search report, in particular the documents cited X and/or Y and corresponding claim references).

10/089990

JC15 PCT/PTO 0 2 APR 2002

SECURITY MODULE  
AND METHOD  
FOR PRODUCTION  
OF  
FORGE-PROOF DOCUMENTS

Jürgen Lang  
-and-  
Bernd Meyer

INTERNATIONAL APPLICATION  
-and-  
Search Report  
-with-  
One (1) Sheet of Drawing

PCT/DE00/03506 ..... IFD: -October 05, 2000-

ACDPA-5002 PWO ..... (10096\*1)  
(POST-1)

"Express Mail" mailing label  
number EL928737461

Date of Deposit  
-APRIL 02, 2002-

I hereby certify that this paper or fee is  
being deposited with the United States Postal  
Service "Express Mail Post Office to  
Addressee" service under 37CFR 1.10 on the  
date indicated above and is addressed to **BOX**  
**PCT, Commissioner for Patents,**  
Washington, D.C. 20231

- J. Lynn Ferry -

(Typed or printed name of person mailing  
paper or fee)

(Signature of person mailing paper or fee)

**THIS PAGE BLANK (USPTO)**



Die Erfindung betrifft ein Sicherungsmodul.

Der Erfindung liegt die Aufgabe zugrunde, ein Sicherungsmodul  
15 zu schaffen, mit dem fälschungssichere Dokumente erzeugt  
werden können.

Erfindungsgemäß wird diese Aufgabe dadurch gelöst, dass ein Sicherungsmodul so gestaltet wird, dass es einen Dateneingang enthält, durch den Informationen in das Sicherungsmodul eingegeben werden können, dass das Sicherungsmodul wenigstens zwei Datenausgänge enthält, wobei durch einen ersten Datenausgang Daten ausgegeben werden können, die an eine Bescheinigungsstelle übertragen werden und wobei durch einen zweiten Datenausgang Daten ausgegeben werden, die auf ein auszugebendes Dokument übertragen werden können, dass das Sicherungsmodul wenigstens zwei Kombinationsmaschinen enthält, wobei eine erste der Kombinationsmaschinen einen Ergebniswert für den ersten Datenausgang erzeugt und wobei eine zweite Kombinationsmaschine einen Ergebniswert für den zweiten Datenausgang erzeugt.

Zur Erhöhung der Datensicherheit ist es zweckmäßig, dass das

Sicherungsmodul so gestaltet wird, dass es einen Geheimnisgenerator enthält, der ein nicht vorhersehbares Geheimnis erzeugt.

- 5 Hierbei ist es besonders vorteilhaft, dass der Geheimnisgenerator mit der ersten Kombinationsmaschine und/oder der zweiten Kombinationsmaschine so verbunden ist, dass ein von dem Geheimnisgenerator erzeugtes Geheimnis in die erste Kombinationsmaschine und/oder die zweite  
10 Kombinationsmaschine eingeht.

- Für eine Anwendung des Sicherungsmoduls in Systemen, in denen eine Abrechnung, insbesondere eine Abrechnung von Leistungen, erfolgt, ist es besonders zweckmäßig, dass das  
15 Sicherungsmodul so gestaltet ist, dass es ein Identifikationsregister enthält, wobei ein Ausgangswert des Identifikationsregisters so mit der ersten Kombinationsmaschine verbunden ist, dass in eine von der ersten Kombinationsmaschine ausgegebene Datenkombination ein  
20 Wert des Identifikationsregisters eingeht.

- Eine weitere Erhöhung der Datensicherheit lässt sich vorteilhafterweise dadurch erzielen, dass das Sicherungsmodul wenigstens eine Verschlüsselungsmaschine enthält, welche  
25 einen Ausgangswert einer der Kombinationsmaschinen verschlüsselt.

- Hierbei ist es zweckmäßig, dass die Verschlüsselungsmaschine mit einem Schlüsselregister verbunden ist, wobei wenigstens  
30 ein in dem Schlüsselregister enthaltener Wert in der Verschlüsselungsmaschine zur Verschlüsselung eingesetzt werden kann.

Eine zweckmäßige Implementation des Sicherungsmoduls zeichnet sich dadurch aus, dass es eine Hash-Maschine enthält.

- Weitere Vorteile, Besonderheiten und zweckmäßige
- 5 Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen und der nachfolgenden Darstellung bevorzugter Ausführungsbeispiele anhand der Zeichnung.

- Die Zeichnung, Fig. 1, zeigt eine Prinzipdarstellung eines
- 10 für die Erstellung fälschungssicherer Dokumente geeigneten Sicherungsmoduls.

- Das in Fig. 1 dargestellte Sicherungsmodul weist einen Dateneingang auf, durch den Informationen in das
- 15 Sicherungsmodul eingegeben werden können.

Das Sicherungsmodul weist ferner zwei Datenausgänge DA1 und DA2 auf.

- 20 Durch den ersten Datenausgang DA1 können Daten ausgegeben werden, die an eine externe Stelle, beispielsweise eine Bescheinigungsstelle, übertragen werden.

- Durch den zweiten Datenausgang DA2 können Daten auf ein
- 25 auszugebendes Dokument übertragen werden.

- Das Sicherungsmodul weist ferner wenigstens zwei Kombinationsmaschinen K1, K2 auf. Die erste Kombinationsmaschine K1 erzeugt einen Ergebniswert für den
- 30 ersten Datenausgang DA1. Die zweite Kombinationsmaschine K2 erzeugt einen Ergebniswert für den zweiten Datenausgang DA2.

Ferner enthält das Sicherungsmodul wenigstens einen

Geheimnisgenerator GG, der ein nicht vorhersehbares Geheimnis erzeugt. Der Geheimnisgenerator ist sowohl mit der ersten Kombinationsmaschine K1 als auch mit der zweiten Kombinationsmaschine K2 verbunden. Die Verbindung zwischen dem Geheimnisgenerator GG und der Kombinationsmaschine K2 erfolgt vorzugsweise über einen Zwischenspeicher.

Der Zwischenspeicher hat vorzugsweise die Funktion, das im Geheimnisgenerator erzeugte Geheimnis temporär zu speichern.

Das Sicherungsmodul enthält ferner ein Identifikationsregister, das so mit der ersten Kombinationsmaschine K1 verbunden ist, dass in eine von der ersten Kombinationsmaschine ausgegebene Datenkombination ein Wert des Identifikationsregisters eingeht.

Eine in dem Sicherungsmodul enthaltene Verschlüsselungsmaschine ist so programmiert, dass sie einen Ausgangswert einer der Kombinationsmaschinen verschlüsselt, im dargestellten Fall der Kombinationsmaschine K1.

Um Speicherplatz zu sparen, ist es zweckmäßig, ein asymmetrisches Schlüsselpaar nach einem geeigneten Sicherheitsstandard wie beispielsweise RSA zur Verschlüsselung und Signatur einzusetzen. Da keine beliebigen, vom Benutzer vorgegebenen Texte in die Verschlüsselung, Signatur und Hashwertbildung einfließen können, ist dieser Schritt zu rechtfertigen.

Die Schlüssellänge beträgt vorzugsweise wenigstens 128 bit, zweckmäßigerweise deutlich mehr, beispielsweise mindestens 1024 bit, RSA.

Die Erzeugung des Hash-Wertes erfolgt vorzugsweise nach dem Standard SHA-1. Die Hash-Maschine verknüpft eingebrachte Daten irreversibel mit einem Geheimnis. Hierdurch entsteht bei wiederholter Verknüpfung derselben Daten in derselben

5 Weise ein identisches Ergebnis, ohne dass Rückschlüsse auf das Geheimnis möglich sind. Vorzugsweise ist das Geheimnis temporär, da hierdurch die Sicherheit gesteigert wird. Dies ist jedoch nicht notwendig. Beispielsweise kann das Geheimnis fest in einem Datenspeicher eingegeben sein.

10

Nachfolgend wird die Funktionsweise des Sicherungsmoduls an dem besonders bevorzugten Beispiel der Freimachung von Briefsendungen erläutert.

15 Das Sicherungsmodul eignet sich jedoch gleichermaßen für andere Verschlüsselungszwecke. Eine Verwendung des Sicherungsmoduls zur Erzeugung fälschungssicherer Dokumente ist besonders zweckmäßig. Der Begriff fälschungssichere Dokumente ist in keiner Weise einschränkend zu verstehen.

20 Neben den beispielhaft dargestellten Freimachungsvermerken kann es sich bei den fälschungssicheren Dokumenten auch um Fahrkarten oder Eintrittskarten handeln. Durch die Möglichkeit, jede einzelne Dokumentenerzeugung auf der Grundlage von individuellen Daten durchzuführen, können auch  
25 einmalige Dokumente wie persönliche Ausweise, Platzkarten oder Listen mit personifizierten Werten erzeugt werden.

Das Sicherungsmodul bearbeitet vorzugsweise individualisierbare Informationen, beispielsweise Zertifikate  
30 und digital signierte Lizenzen.

Bei einem bevorzugten Beispiel eines Einsatzes für die Freimachung von Briefen im Bereich der Deutschen Post AG

geschieht dies wie folgt:

Eine digitale Signatur ist ein mit einem privaten  
Signatur Schlüssel erzeugtes Siegel zu digitalen Daten, das  
5 mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit  
einem Signatur Schlüssel-Zertifikat versehen ist, den Inhaber  
des Signatur Schlüssels und die Unverfälschtheit der Daten  
erkennen lässt (vgl. SigG §2, Abs. 1). Unter Benutzung der  
hier verwandten Terminologie ist eine Prüfstelle in der Lage,  
10 die digitale Signatur eines Dokumentherstellers und somit  
sowohl dessen Identität als auch die Unverfälschtheit der im  
Dokument enthaltenen Daten zu prüfen, wenn ihr der  
öffentliche Signatur Schlüssel des Dokumentherstellers, der  
mit einem Signatur Schlüssel-Zertifikat versehen ist, zur  
15 Verfügung steht.

Jedes hergestellte Sicherungsmodul wird von dem  
Kundensystemhersteller „digital lizenziert“. Die  
Bescheinigungsstelle erstellt zur Kommunikation mit den  
20 Sicherungsmodulen eine eigene signierte Kommunikationslizenz  
im gleichen Format.

Die Zertifizierung und signierte Lizenzierung erfolgen  
vorzugsweise wie folgt:

25

Das Sicherungsmodul erzeugt intern ein Schlüsselpaar, dessen  
öffentlicher Schlüssel  $P_{SB}$  (Public Key) unter Benutzung des  
privaten Signatur Schlüssels des Kundensystemanbieters  $S_I$   
(Issuer) digital lizenziert wird. Der öffentliche Schlüssel  
30 des Kundensystemanbieters  $P_I$  ist ebenso wie der öffentliche  
Schlüssel der Bescheinigungsstelle von der  
Zertifizierungsstelle (CA) • erstellt und zertifiziert und

steht dort zur Prüfung zur Verfügung.

Insgesamt werden im System folgende Schlüssel, Zertifikate und signierte Lizenzen verwendet.

5

In dem Sicherungsmodul stehen ein privater Schlüssel des Sicherungsmoduls, ein öffentlicher Schlüssel des Sicherungsmoduls und eine durch den Kundensystemanbieter (Issuer) signierte Lizenz des öffentlichen Schlüssels des

10

Sicherungsmoduls.

In der Bescheinigungsstelle stehen vorzugsweise mindestens ein privater Schlüssel der Bescheinigungsstelle und ein öffentlicher Schlüssel der Bescheinigungsstelle zur

15

Verfügung.

Das Sicherungsmodul prüft die Gültigkeit der signierten Lizenz, beispielsweise durch Kontaktierung einer Zertifizierungsstelle.

20

Die Bescheinigungsstelle prüft die Gültigkeit der signierten Lizenz eines Sicherungsmoduls - und somit die Identität des Kundensystemanbieters (Issuer) über die Identität der per Attributeintrag im Zertifikat für den Kundensystemanbieter

25

verantwortlichen natürlichen Person - durch Kontaktierung der Zertifizierungsstelle.

Der Herausgeber der Signaturkarten stellt sicher, dass entsprechende Attribute (z.B. Prokura zur Ausgabe von

30

Lizenzen für Sicherungsmodule) ausschließlich in Abstimmung mit der Stelle, bei der die fälschungssicheren Dokumente eingereicht werden, vergeben werden.

Ein regulärer Austausch des Schlüsselpaares des Sicherungsmoduls ist nicht notwendig, jedoch möglich. Die vorgesehene Gültigkeitsdauer der Schlüssel ist möglichst lang, um die Benutzerfreundlichkeit zu erhöhen. Die

- 5 Gültigkeitsdauer der Schlüssel des Sicherungsmoduls beträgt vorzugsweise mehrere Monate bis Jahre, wobei Werte zwischen drei Monaten und 15 Jahren infrage kommen. Vorzugsweise beträgt die Gültigkeitsdauer zwischen 3 Jahren und 10 Jahren, wobei sich etwa 6 Jahre besonders eignen.

10

Der Kundensystemhersteller ist berechtigt, die Schlüssel, mit denen er die Lizenzen der ausgegebenen Sicherungsmodule digital lizenziert, jederzeit zu wechseln. Der Kundensystemhersteller ist verpflichtet, die

- 15 Signaturschlüssel, mit denen er die Lizenzen der ausgegebenen Sicherungsmodule digital signiert, nach spätestens einem Jahr zu wechseln und hierbei den alten Signaturschlüssel sperren zu lassen. Der Kundensystemhersteller kennzeichnet die Signaturschlüssel in Abstimmung mit der Bescheinigungsstelle.

20

Eine zur Prüfung der fälschungssicheren Dokumente berechtigte Stelle lehnt Transaktionen bei Feststellung einer Korruption eines Schlüssels ab. Bei einem Einsatz des Sicherungsmoduls zur Herstellung fälschungssicherer

- 25 Postwertzeichen ist die zur Überprüfung der Dokumente berechtigte Stelle der Postdienstbetreiber, beispielsweise die Deutsche Post AG. In diesem Fall hat eine Korruption eines Schlüssels eines Kundensystemanbieters eine sofortige postseitige Ablehnung jeglicher Transaktionen mit
- 30 Sicherungsmodulen der Kundensystemhersteller zur Folge, deren signierte Lizenzen mit diesem Schlüssel hergestellt wurden.

Die Verwaltung der Schlüssel der Zertifizierungsstelle



erfolgt entsprechend massgeblicher gesetzlicher und verwaltungsrechtlicher Bestimmungen. In Deutschland sind dies das Signaturgesetz SigG und die Signaturverordnung SigV. Eine weitere Erhöhung der Sicherheit durch Einbeziehung interner Bearbeitungs Vorschriften ist möglich.

Die Schlüssel der Bescheinigungsstelle können jederzeit gewechselt werden, ohne dass hierbei Änderungen in den Kundensystemen erforderlich werden.

10

Nachfolgend wird ein Bescheinigungsverfahren anhand eines Einsatzes von symmetrischen Schlüsseln der Bescheinigungsstelle erläutert.

15 Symmetrische Schlüssel erlauben eine sehr schnelle Ver- und Entschlüsselung. Ein Einsatz von symmetrischen Schlüsseln setzt voraus, dass der Schlüssel des Senders und der Schlüssel des Empfängers übereinstimmen. Bei einer Kommunikation zwischen der Bescheinigungsstelle und einer  
20 Vielzahl von Kundensystemen können symmetrische Schlüssel dann eingesetzt werden, wenn die Bescheinigungsstelle über ausreichende Speicherkapazität für die einzelnen Schlüssel verfügt, die zu den jeweiligen Kundensystemen passen.

25 Ein Einsatz von asymmetrischen Schlüsseln sieht hingegen vor, dass der Sender die Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und dass der Empfänger die Nachricht mit seinem privaten Schlüssel entschlüsselt.

30 Je nach Einsatzgebiet ist ein Einsatz von symmetrischen oder von asymmetrischen Schlüsseln vorzusehen. Die dargestellten Verfahren können jedoch grundsätzlich sowohl mit symmetrischen als auch mit asymmetrischen Schlüsseln

erfolgen.

#### Sicherheitsrelevante Aufgaben des Sicherungsmoduls

- 5 Das Sicherungsmodul muss zur Initialisierung, zur Kommunikation mit der Bescheinigungsstelle und zur Deaktivierung im Wesentlichen folgende Aufgaben erfüllen:

##### Schlüsselerzeugung

- 10 Erzeugung und Speicherung eines asymmetrischen Schlüsselpaars innerhalb des Sicherungsmoduls.

##### Ausgabe des öffentlichen Schlüssels

- 15 Ausgabe des erzeugten öffentlichen Schlüssels im Rahmen der digitalen Signatur der Lizenz durch den Kundensystemanbieter (Issuer). Der private Schlüssel darf das Sicherungsmodul niemals verlassen.

##### Zertifikatspeicherung

- 20 Dauerhafte Speicherung des eigenen öffentlichen Schlüssels, beziehungsweise der eigenen signierten Lizenz im Rahmen der Initialisierung.

##### Signaturerzeugung

- 25 Erzeugung einer digitalen Signatur unter Verwendung des eigenen privaten Signaturschlüssels.

##### Signaturprüfung:

- 30 Prüfung der digitalen Signatur eines Bescheinigungsmoduls der Bescheinigungsstelle unter Verwendung der signierten Lizenz der Bescheinigungsstelle und deren Zertifikat nach einer geeigneten Sicherheitsnorm, beispielsweise dem SigG.

### Zertifikatprüfung

Prüfung eines Zertifikats durch Anfrage bei der Zertifizierungsstelle.

### 5 Temporäre Zertifikatspeicherung

Temporäre Speicherung eines Zertifikats oder einer signierten Lizenz im Rahmen einer Kommunikationssitzung.

### Asymmetrische Verschlüsselung

- 10 Verschlüsselung von Daten mit einem verifizierten öffentlichen Schlüssel eines Kommunikationspartners.

### Asymmetrische Entschlüsselung

- 15 Entschlüsselung von Daten mit dem eigenen privaten Schlüssel, die mit dem eigenen öffentlichen Schlüssel verschlüsselt wurden.

### Zufallszählerzeugung

- 20 Erzeugung und dauerhafte Speicherung einer nachweisbar qualitativ hochwertigen Zufallszahl in einem Zahlenraum von mindestens 16 byte.

### Speicherung eines Sitzungsschlüssels

- 25 Temporäre Speicherung eines Sitzungsschlüssels mit einer Länge von 16 byte.

Speicherung von zwei Identifikationsnummern des Ladevorganges  
Speicherung der jeweils zwei neuesten Identifikationsnummern mit einer Länge von jeweils 16 byte.

30

Speicherung des aktuellen Registerwerts der Wertbörse  
Speicherung der Währung und des Betrags, der aktuell zur Herstellung von Freimachungsvermerken verwendet werden kann;

„Descending Register“.

Speicherung des aufsteigenden Registerwerts

Speicherung aller insgesamt mit dem Sicherungsmodul

- 5 freigemachten Beträge, vorzugsweise in einer einheitlichen Währung, beispielsweise dem Euro; „Ascending Register“.

Benutzeridentifikation

Persönliche Identifikation des für bestimmte

- 10 Nutzungsmöglichkeiten berechtigten Benutzers des Sicherungsmoduls durch Verwendung einer mit dem eigenen öffentlichen Schlüssel zu verschlüsselnden PIN.

Statusausgabe der Identifikationsnummer des Ladevorganges

- 15 Ausgabe der Gültigkeit des aktuellen Ladesystems an das Kundensystem ohne die Möglichkeit der Änderung durch das Kundensystem.

Statusausgabe des Registerwerts der Wertbörse

- 20 Ausgabe des aktuellen verfügbaren Börsenwerts an das Kundensystem ohne die Möglichkeit der Änderung durch das Basissystem.

Hash-Bildung der sendungsspezifischen Daten

- 25 Bildung eines Hash-Wertes, beispielsweise nach SHA-1 von den vom Kundensystem übermittelten sendungsspezifischen Daten und der gespeicherten Zufallszahl.

- 30 Verminderung von Registerwerten einer Wertbörse

Vorzugsweise arbeitet das Sicherungsmodul mit einer digitalen Wertbörse zusammen. Diese Wertbörse kann in das Sicherungsmodul integriert sein oder separat untergebracht

- werden. Eine separate Unterbringung erfolgt beispielsweise in einer digitalen Brieftasche (Digital-Wallet). Durch die Speicherung wird sichergestellt, dass nur tatsächlich vorhandene Beträge benutzt werden. Bei der Benutzung, bei der
- 5 beispielsweise eine Hash-Wert-Bildung erfolgt, wird der Betrag und damit auch der ihm zugeordnete Registerwert verringert.

- Digitale Signatur der sendungsspezifischen Daten
- 10 Bildung und Ausgabe der Digitalen Signatur der sendungsspezifischen Daten bei jeder Hash-Bildung der sendungsspezifischen Daten.

#### Fehlerprotokollierung

- 15 Protokollierung der Aktivität sowie gültiger und ungültiger Kommunikationsversuche mit dem Sicherungsmodul.

#### Selbsttest

- Durchführung eines Selbsttests bei jeder Aktivierung.
- 20

#### Deaktivierung

- Deaktivierung des Sicherungsmoduls nach Identifikation und Aufforderung durch einen Operator.

- 25 Sicherheitsniveau durch Security Level nach FIPS PUB 140

- Ziel des Sicherungsmoduls ist es, innerhalb eines Kundensystems die Vertraulichkeit und Integrität von Informationen, die im Sicherungsmodul gespeichert und
- 30 verarbeitet werden, zu gewährleisten. Zur Erlangung eines einheitlichen Sicherheitsniveaus bei unterschiedlichen Kundensystemen und unterschiedlichen Sicherungsmodulen ist die Übereinstimmung mit und Zertifizierung nach einer vorher

festgelegten Sicherheitsstufe, beispielsweise entsprechend einer durch FIPS PUB 140 vorgegebenen Sicherheitsstufe (FIPS PUB 140: "Security Level"), zweckmäßig.

- 5 Die Anwendung von FIPS PUB 140, Security Level 4, ist besonders vorteilhaft.

Die zur Durchführung empfohlene Sicherheitsstufe ist FIPS PUB 140, Security Level 3, weil hierdurch eine hohe  
10 Datensicherheit mit einem geringen Handhabungsaufwand verbunden werden.

Es ist besonders zweckmäßig, dass das System über FIPS PUB 140-1 hinausgehende Anforderungen erfüllt.

15

Zu einer weiteren Erhöhung der Datensicherheit ist es zweckmäßig, die sicherheitsrelevanten Prozesse des Kundensystems wie folgt durchzuführen:

- 20 Die Herstellung und Initialisierung des Sicherungsmoduls erfolgt in einer abgeschirmten Umgebung nach einem mit der Deutschen Post abgestimmten Sicherheitsstandard. Das Risiko der Korruption des zum Einsatz kommenden  
Signaturschlüssels zur Erzeugung der signierten Lizenzen der  
25 hergestellten Sicherheitsmodule wird durch Überprüfungen minimiert. Bei der Herstellung werden ein Schlüsselpaar erzeugt, ein öffentlicher Schlüssel zur Erzeugung der signierten Lizenz durch den Kundensystemanbieter ausgegeben, eine signierte Lizenz des Sicherheitsmoduls (inklusive  
30 Sicherheitsmodul-ID) im Sicherheitsmodul gespeichert und der Attributeintrag in einem eingesetzten Zertifikat gespeichert.

## Aktivierung des Sicherungsmoduls durch das Kundensystem

Um vom Kundensystem aus das Sicherungsmodul zu aktivieren, wird dieses aufgefordert, seine signierte Lizenz (inklusive  
5 seines öffentlichen Schlüssels  $P_{SB}$ ) sowie eine Zufallszahl  $X_{auth}$  mit einer Länge von 16 byte an das Kundensystem zu übergeben. (Die Zufallszahl dient insbesondere dann zur Absicherung von Replay-Attacken, wenn zwischen Tastatur des Kundensystems und Sicherungsmodul ein ungesicherter  
10 Übertragungswert liegt, etwa bei Internet Lösungen mit zentralem Sicherungsmodul-Server im Internet und dezentralen PCs als Eingabeterminals für Login-Informationen wie zum Beispiel PIN).

## 15 Fehlerbehandlung

Werden signierte Lizenz und Zufallszahl mehrmals, beispielsweise dreimal hintereinander angefordert, ohne dass anschließend Login-Daten vom Kundensystem an das  
20 Sicherungsmodul übertragen werden, muss dies im Sicherungsmodul protokolliert werden. Bei diesem Status darf ausschließlich eine anschließende Verbindung mit der Bescheinigungsstelle zur Fehlerbehebung mit Übertragung des Protokollstatus, nicht jedoch die Herstellung von  
25 fälschungssicheren Dokumenten wie Eintrittskarten oder Freimachungsvermerken, möglich sein.

Nach der Authentisierung des Kundensystems/Kunden liest das Sicherungsmodul die aktuelle Identifikationsnummer des  
30 Ladevorganges, die vorhergehende Identifikationsnummer, den aktuellen Wertbetrag und die Gültigkeit des Wertes und übergibt sie an das Basissystem. Eine Veränderung dieser Werte darf durch diesen Benutzer (FIPS PUB 140: role) in

dieser Nutzungsmöglichkeit Benutzer (FIPS PUB 140: service)  
nicht bestehen.



## Patentansprüche:

1. Sicherungsmodul, d a d u r c h g e -  
5 k e n n z e i c h n e t, dass es einen  
Dateneingang enthält, durch den Informationen in das  
Sicherungsmodul eingegeben werden können, dass das  
Sicherungsmodul wenigstens zwei Datenausgänge enthält,  
10 wobei durch einen ersten Datenausgang Daten ausgegeben  
werden können, die an eine Bescheinigungsstelle  
übertragen werden und wobei durch den zweiten  
Datenausgang Daten ausgegeben werden, die auf ein  
auszugebendes Dokument übertragen werden können, mit  
15 wenigstens zwei Kombinationsmaschinen (K1, K2), wobei  
eine erste der Kombinationsmaschinen (K1) einen  
Ergebniswert für den ersten Datenausgang erzeugt und  
wobei eine zweite Kombinationsmaschine (K2) einen  
Ergebniswert für den zweiten Datenausgang erzeugt.
- 20 2. Sicherungsmodul nach Anspruch 1, d a d u r c h  
g e k e n n z e i c h n e t, dass es einen  
Geheimnisgenerator enthält, der ein nicht vorhersehbares  
Geheimnis erzeugt.
- 25 3. Sicherungsmodul nach Anspruch 2, d a d u r c h  
g e k e n n z e i c h n e t, dass der  
Geheimnisgenerator mit der ersten Kombinationsmaschine  
und/oder der zweiten Kombinationsmaschine so verbunden  
ist, dass ein von dem Geheimnisgenerator erzeugtes  
30 Geheimnis in die erste Kombinationsmaschine (K1)  
und/oder die zweite Kombinationsmaschine (K2) eingeht.
4. Sicherungsmodul nach einem oder mehreren der

vorangegangenen Ansprüche, d a d u r c h  
g e k e n n z e i c h n e t, dass es ein  
Identifikationsregister enthält, wobei ein Ausgangswert  
des Identifikationsregisters so mit der ersten  
5 Kombinationsmaschine (K1) verbunden ist, dass in eine  
von der ersten Kombinationsmaschine ausgegebene  
Datenkombination ein Wert des Identifikationsregisters  
eingeht.

- 10 5. Sicherungsmodul nach einem oder mehreren der  
vorangegangenen Ansprüche, d a d u r c h  
g e k e n n z e i c h n e t, dass es wenigstens  
eine Verschlüsselungsmaschine enthält, welche einen  
Ausgangswert einer der Kombinationsmaschinen (K1)  
15 verschlüsselt.

6. Sicherungsmodul nach Anspruch 5, d a d u r c h  
g e k e n n z e i c h n e t, dass die  
Verschlüsselungsmaschine mit einem Schlüsselregister  
20 verbunden ist, wobei wenigstens ein in dem  
Schlüsselregister enthaltener Wert in der  
Verschlüsselungsmaschine zur Verschlüsselung eingesetzt  
werden kann.

- 25 7. Sicherungsmodul nach einem oder mehreren der  
vorangegangenen Ansprüche, d a d u r c h  
g e k e n n z e i c h n e t, dass es eine Hash-  
Maschine enthält.

- 30 8. Verfahren zur Erstellung fälschungssicherer Dokumente,  
wobei Eingangsdaten in einen Dateneingang eines  
Sicherungsmoduls eingegeben werden und wobei in dem  
Sicherungsmodul zur Identifizierung einzelner Dokumente

dienende Informationen erzeugt werden, d a -  
d u r c h g e k e n n z e i c h n e t,  
dass die Eingangsdaten in einen Dateneingang eines  
Sicherungsmoduls eingegeben werden, dort mit ein  
5 Geheimnis repräsentierenden Daten kombiniert werden und  
dass das Geheimnis in einem von dem Kombinieren  
getrennten Verarbeitungsschritt weiter verarbeitet wird  
und dass Daten aus der Kombination der das Geheimnis  
repräsentierenden Daten und der Eingangsdaten gewonnen  
10 werden.

9. Verfahren nach Anspruch 8, d a d u r c h  
g e k e n n z e i c h n e t, dass das Geheimnis  
durch einen ersten Datenausgang ausgegeben wird und dass  
15 die Daten, die aus der Kombination der das Geheimnis  
repräsentierenden Daten und der Eingangsdaten gewonnen  
werden, an einem zweiten Datenausgang ausgegeben werden.

10. Verfahren nach einem oder mehreren der Ansprüche 8 oder  
20 9, d a d u r c h g e k e n n -  
z e i c h n e t, dass die Kombination der das  
Geheimnis repräsentierenden Daten und der Eingangsdaten  
in einer zweiten Kombinationsmaschine (K2) erfolgt.

25 11. Verfahren nach Anspruch 10, d a d u r c h  
g e k e n n z e i c h n e t, dass die das  
Geheimnis repräsentierenden Daten und die Eingangsdaten  
irreversibel miteinander verknüpft werden, wobei die  
irreversible Verknüpfung so erfolgt, dass ausschließlich  
30 bei wiederholter Verknüpfung derselben Daten in  
derselben Weise ein identisches Ergebnis entsteht ohne  
dass Rückschlüsse auf das temporäre Geheimnis möglich  
sind.

12. Verfahren nach einem oder mehreren der Ansprüche 8 bis  
11, d a d u r c h g e k e n n -  
z e i c h n e t, dass die weitere Verknüpfung der  
5 das Geheimnis repräsentierenden Daten unter Einbeziehung  
von Daten eines Identifikationsregisters erfolgt.

13. Verfahren nach Anspruch 12, d a d u r c h  
g e k e n n z e i c h n e t, dass das Ergebnis  
10 der Kombination der Daten, die das Geheimnis  
repräsentieren und der Daten des  
Identifikationsregisters (ID) in einer  
Verschlüsselungsmaschine verschlüsselt wird.

15 14. Verfahren nach Anspruch 13, d a d u r c h  
g e k e n n z e i c h n e t, dass die  
Verschlüsselung unter Einbeziehung eines Schlüssels  
erfolgt, dessen Wert in einem Schlüsselregister (SR)  
gespeichert ist.

20

15. Verfahren nach einem oder mehreren der Ansprüche 8 bis  
14, d a d u r c h g e k e n n -  
z e i c h n e t, dass die Daten, die aus dem ersten  
Datenausgang ausgegeben werden, an eine  
25 Bescheinigungsstelle übertragen werden.

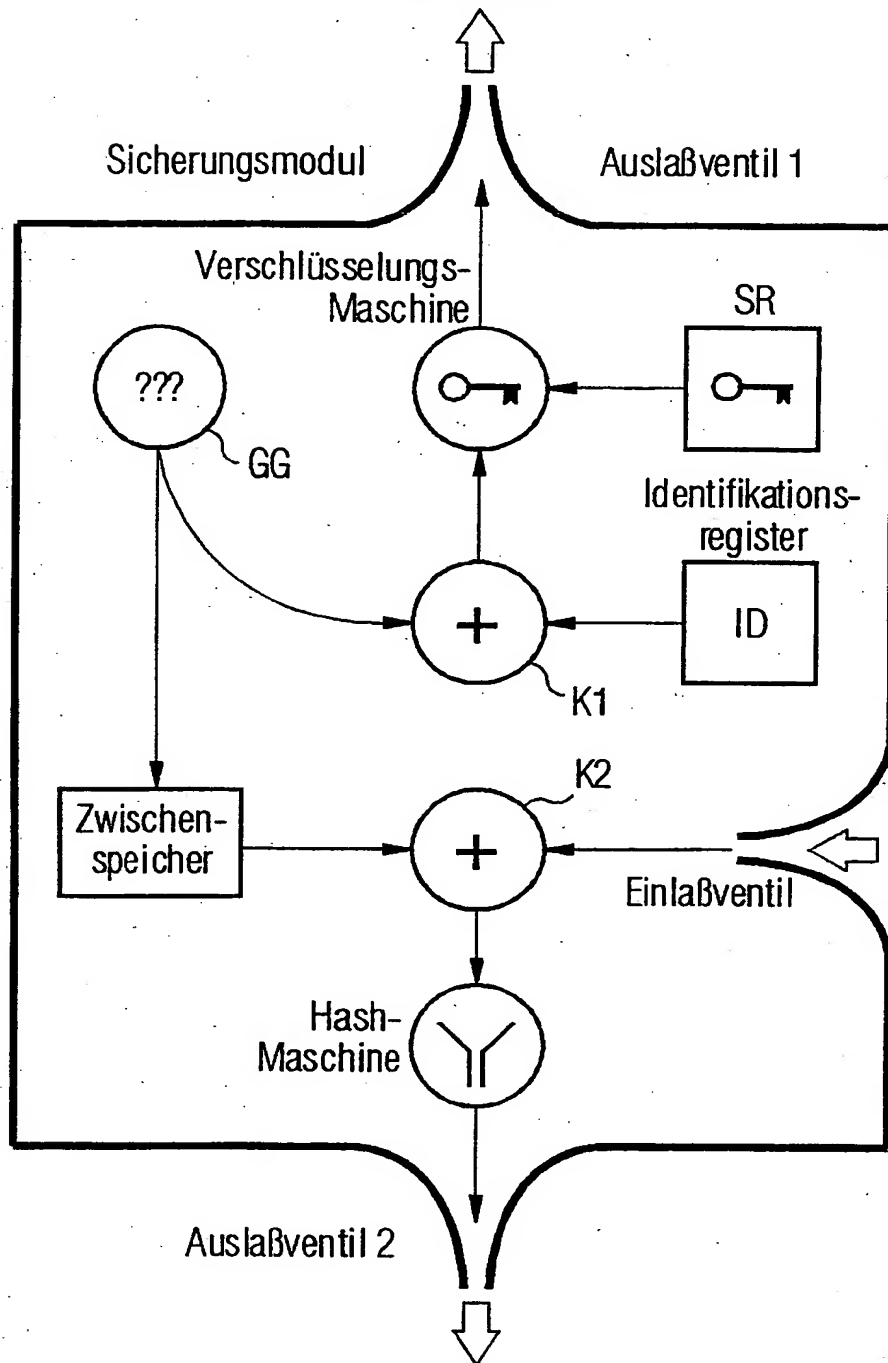
16. Verfahren nach Anspruch 15, d a d u r c h  
g e k e n n z e i c h n e t, dass die  
Bescheinigungsstelle die Daten mit einem weiteren  
30 Schlüssel verknüpft.

17. Verfahren nach einem oder mehreren der Ansprüche 8 bis  
16, d a d u r c h g e k e n n -

z e i c h n e t, dass die Daten, die aus dem zweiten Datenausgang ausgegeben werden als fälschungssichere Informationen auf die zu erstellenden fälschungssicheren Dokumente ausgegeben werden.

**THIS PAGE BLANK (USPTO)**

Verfahren und System zur Erstellung  
fälschungssicherer Dokumente  
Zeichnung 1



**THIS PAGE BLANK (USPTO)**

**"Express Mail" mailing label  
number \_\_\_\_\_  
Date of Deposit \_\_\_\_\_**

**I hereby certify that this paper or fee is  
being deposited with the United States Postal  
Service "Express Mail Post Office to  
Assessor" service under 37CFR 1.10 on the  
date indicated above and is addressed to the  
Assistant Commissioner for Patents,  
Washington, D.C. 20231**

**(Typed or printed name of person mailing  
paper or fee) \_\_\_\_\_**

**(Signature of person mailing paper or fee) \_\_\_\_\_**



(12) NACH DEM VERTRAG FÜR DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES  
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum  
Internationales Büro



(43) Internationales Veröffentlichungsdatum  
12. April 2001 (12.04.2001)

PCT

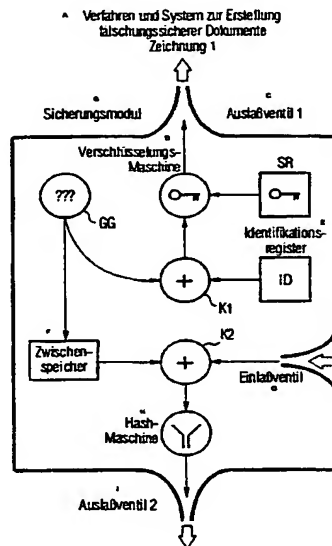
(10) Internationale Veröffentlichungsnummer  
WO 01/25879 A3

- (51) Internationale Patentklassifikation<sup>7</sup>: G07B 17/00 (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): DEUTSCHE POST AG [DE/DE]; Heinrich-von-Stephan-Strasse 1, 53175 Bonn (DE).
- (21) Internationales Aktenzeichen: PCT/DE00/03506
- (22) Internationales Anmeldedatum: 5. Oktober 2000 (05.10.2000) (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): LANG, Jürgen [DE/DE]; Schau ins Land 15, 51429 Bergisch Gladbach (DE). MEYER, Bernd [DE/DE]; Zum Stöckerhof 2 c, 53639 Königswinter (DE).
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch (74) Anwalt: JOSTARNDT, Hans-Dieter; Eupener Strasse 266, 52076 Aachen (DE).
- (30) Angaben zur Priorität:  
199 48 319.1 7. Oktober 1999 (07.10.1999) DE (81) Bestimmungsstaaten (national): AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE,  
100 20 561.5 27. April 2000 (27.04.2000) DE

[Fortsetzung auf der nächsten Seite]

(54) Title: SECURITY MODULE AND METHOD FOR PRODUCTION OF FORGE-PROOF DOCUMENTS

(54) Bezeichnung: SICHERUNGSMODUL UND VERFAHREN ZUR ERSTELLUNG FÄLSCHUNGSSICHERER DOKUMENTE



A. METHOD AND SYSTEM FOR THE GENERATION OF FORGE-PROOF DOCUMENTS  
B. INPUT VALVE  
C. OUTPUT VALVE 1  
D. OUTPUT VALVE 2  
E. IDENTIFICATION REGISTER  
F. INTERMEDIATE MEMORY  
G. HASH MACHINE  
H. ENCRYPTION MACHINE  
I. OUTPUT VALVE 3

(57) Abstract: The invention relates to a security module characterized in that said module contains a data input port via which information can be inputted into the security modul. The security module has at least two data output ports whereby data can be outputted via a first data output port and transferred to an authentication unit and whereby data can be outputted via a second data output port. Said data can be transferred to a document to be exported. Said security module has at least two combination machines. A first combination machine generates a first result value for a first data output and a second combination machine generates a result value for the second data output. The invention relates to the use of a security module for generating forge-proof documents.

(57) Zusammenfassung: Erfindungsgemäß zeichnet sich das Sicherungsmodul dadurch aus, dass es einen Dateneingang enthält, durch den Informationen in das Sicherungsmodul eingegeben werden können, dass das Sicherungsmodul wenigstens zwei Datenausgänge enthält, wobei durch einen ersten Datenausgang

[Fortsetzung auf der nächsten Seite]

WO 01/25879 A3



ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW.

**Veröffentlicht:**

- mit internationalem Recherchenbericht
- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen

(84) **Bestimmungsstaaten (regional):** ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

(88) **Veröffentlichungsdatum des internationalen Recherchenberichts:**

21. März 2002

*Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.*

Daten ausgegeben werden können, die an eine Bescheinigungsstelle übertragen werden und wobei durch einen zweiten Datenausgang Daten ausgegeben werden, die auf ein auszugebendes Dokument übertragen werden können, mit wenigstens zwei Kombinationsmaschinen, wobei eine erste der Kombinationsmaschinen einen Ergebniswert für den ersten Datenausgang erzeugt und wobei eine zweite Kombinationsmaschine einen Ergebniswert für den zweiten Datenausgang erzeugt. Die Erfindung betrifft ferner den Einsatz des Sicherungsmoduls zur Erstellung fälschungssicherer Dokumente.

## INTERNATIONAL SEARCH REPORT

International Application No.

PCT/D/03506

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G07B17/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, WPI Data, PAJ

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 331 352 A (ALCATEL BUSINESS SYSTEMS ;ALCATEL NV (NL)) 6 September 1989 (1989-09-06) column 1, line 1 - line 5 column 2, line 8 - line 45 column 4, line 34 -column 5, line 5 column 6, line 10 - line 21 ----	1-17
Y	AKL S G ET AL: "DIGITAL SIGNATURES: A TUTORIAL SURVEY" COMPUTER, IEEE COMPUTER SOCIETY, LONG BEACH., CA, US, US, vol. 16, no. 2, February 1983 (1983-02), pages 15-24, XP000946230 ISSN: 0018-9162 page 19, right-hand column -page 23, left-hand column ----- -/--	1-17

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

## \* Special categories of cited documents:

\*A\* document defining the general state of the art which is not considered to be of particular relevance

\*E\* earlier document but published on or after the international filing date

\*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

\*O\* document referring to an oral disclosure, use, exhibition or other means

\*P\* document published prior to the international filing date but later than the priority date claimed

\*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

\*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

\*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

\*&amp;\* document member of the same patent family

Date of the actual completion of the international search

12 December 2001

Date of mailing of the international search report

09/01/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Carnerero Álvaro, F

## INTERNATIONAL SEARCH REPORT

International Application No.

1/DE 00/03506

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, A	<p>HUHNLEIN D ; MERKLE J: "Secure and cost efficient electronic stamps" SECURE NETWORKING - CORE SECURE'99, PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.1740), 'Online! 30 November 1999 (1999-11-30) - 2 December 1999 (1999-12-02), pages 94-100, XP002185463 Dusseldorf, Germany ISBN: 3-540-66800-4 Retrieved from the Internet: &lt;URL:http://citeseer.nj.nec.com/cs&gt; 'retrieved on 2001-12-12! the whole document</p> <p>----</p>	1-17
A	<p>"Information Based Indicia Program Postal Security Device Specification" INFORMATION BASED INDICIA PROGRAM. POSTAL SECURITY DEVICE SPECIFICATION, XX, XX, 13 June 1996 (1996-06-13), pages 1-41, XP002137734 the whole document</p> <p>-----</p>	1-17

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/03506

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0331352	A	06-09-1989	AT 107057 T	15-06-1994
			DE 68915816 D1	14-07-1994
			DE 68915816 T2	19-01-1995
			EP 0331352 A2	06-09-1989
			US 4934846 A	19-06-1990
<hr/>				

**THIS PAGE BLANK (USPTO)**

ACDPA-5002 PWO  
(Post-1)

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTRECHTS

## PCT

### INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>ACDPA5002PWO</b>	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen <b>PCT/DE 00/ 03506</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>05/10/2000</b>	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) <b>07/10/1999</b>

Anmelder

**DEUTSCHE POST AG et al.**

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.



Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

#### 1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.



Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das



in der internationalen Anmeldung in schriftlicher Form enthalten ist.



zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.



bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.



bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.



Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.



Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

#### 4. Hinsichtlich der Bezeichnung der Erfindung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut von der Behörde wie folgt festgesetzt:

#### 5. Hinsichtlich der Zusammenfassung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

#### 6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1



wie vom Anmelder vorgeschlagen



weil der Anmelder selbst keine Abbildung vorgeschlagen hat.



weil diese Abbildung die Erfindung besser kennzeichnet.



keine der Abb.

**THIS PAGE BLANK (USPTO)**



## INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE 00/03506

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES  
IPK 7 G07B17/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)  
IPK 7 G07B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, INSPEC, WPI Data, PAJ

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP 0 331 352 A (ALCATEL BUSINESS SYSTEMS ;ALCATEL NV (NL)) 6. September 1989 (1989-09-06) Spalte 1, Zeile 1 - Zeile 5 Spalte 2, Zeile 8 - Zeile 45 Spalte 4, Zeile 34 - Spalte 5, Zeile 5 Spalte 6, Zeile 10 - Zeile 21 ---	1-17
Y	AKL S G ET AL: "DIGITAL SIGNATURES: A TUTORIAL SURVEY" COMPUTER, IEEE COMPUTER SOCIETY, LONG BEACH., CA, US, US, Bd. 16, Nr. 2, Februar 1983 (1983-02), Seiten 15-24, XP000946230 ISSN: 0018-9162 Seite 19, rechte Spalte -Seite 23, linke Spalte --- -/--	1-17



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

- \*A\* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
- \*E\* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
- \*L\* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
- \*O\* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
- \*P\* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

\*T\* Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

\*X\* Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

\*Y\* Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

\*Z\* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

12. Dezember 2001

Absendedatum des internationalen Recherchenberichts

09/01/2002

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Carnerero Álvaro, F

**THIS PAGE BLANK (USPTO)**

## C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,A	<p>HUHNLEIN D ; MERKLE J: "Secure and cost efficient electronic stamps" SECURE NETWORKING - CORE SECURE'99, PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.1740), 'Online! 30. November 1999 (1999-11-30) - 2. Dezember 1999 (1999-12-02), Seiten 94-100, XP002185463 Dusseldorf, Germany ISBN: 3-540-66800-4 Gefunden im Internet: &lt;URL:http://citeseer.nj.nec.com/cs&gt; 'gefunden am 2001-12-12! das ganze Dokument</p> <p>---</p>	1-17
A	<p>"Information Based Indicia Program Postal Security Device Specification" INFORMATION BASED INDICIA PROGRAM. POSTAL SECURITY DEVICE SPECIFICATION, XX, XX, 13. Juni 1996 (1996-06-13), Seiten 1-41, XP002137734 das ganze Dokument</p> <p>-----</p>	1-17

**THIS PAGE BLANK (USPTO)**

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

CT/DE 00/03506

Formblatt PCT/ISA/210 (Anhang Patentfamilie)(Juli 1992)

**THIS PAGE BLANK (USPTO)**